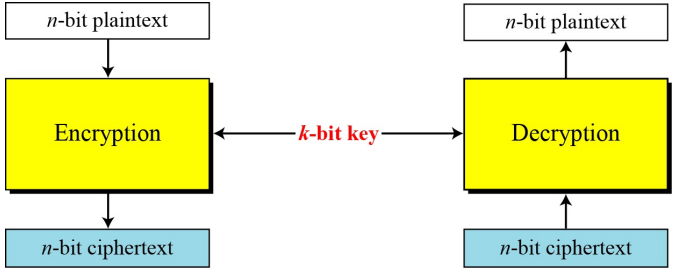
Mode of Operation 운영모드

Jong Hwan Park

Mode of Operation

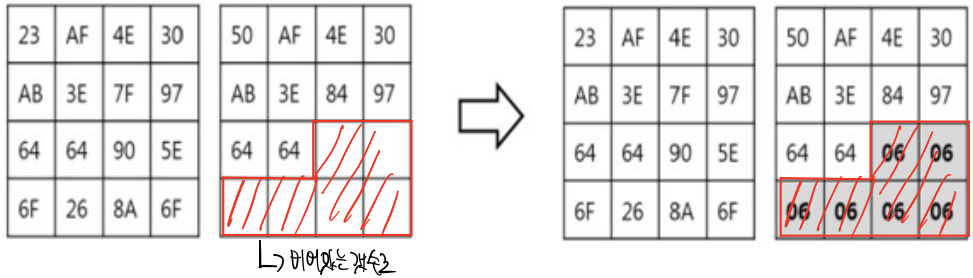
- A way of encrypting arbitrary-length messages using block cipher (3DES or AES)
  - 64 bits block (3DES) and 128 bits block (AES) ⇒ 문제는 이 block의 크기가 작다. → message의 길이가 크면?
  - How can we encrypt messages larger than the block length?



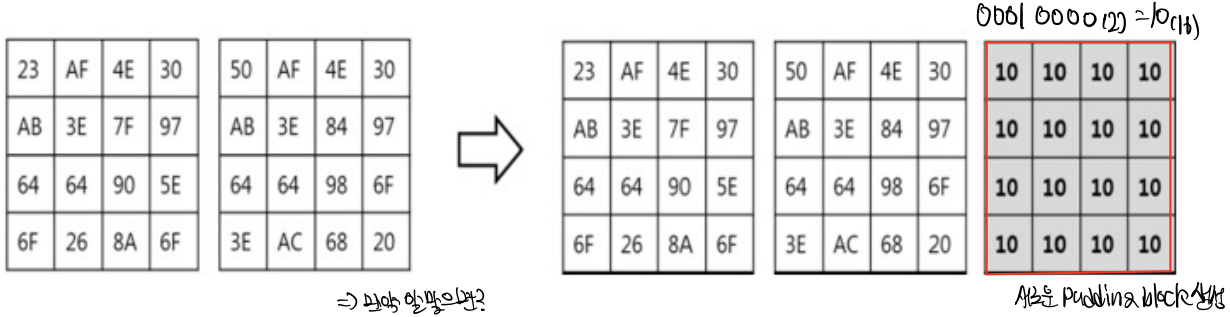
- Five (representative) modes
  - Electronic Code Book (ECB) mode
  - Cipher Block Chaining (CBC) mode
  - Cipher Feedback (CFB) mode
  - Output Feedback (OFB) mode
  - Counter (CTR) mode

Padding

- PKCS#7 padding block 단위의 완성화를 위한 규칙
  - Byte padding
    - If |m| is not a multiple of block size

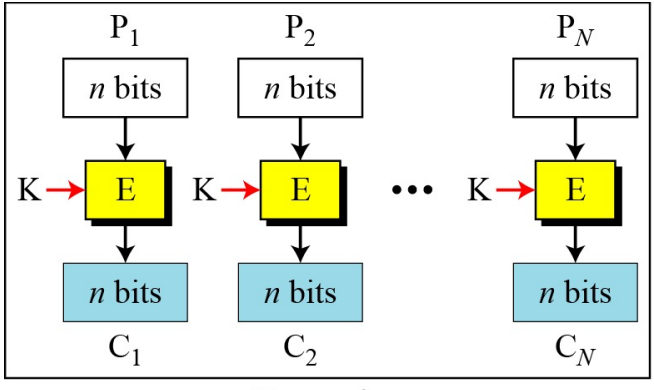


    - If |m| is a multiple of block size

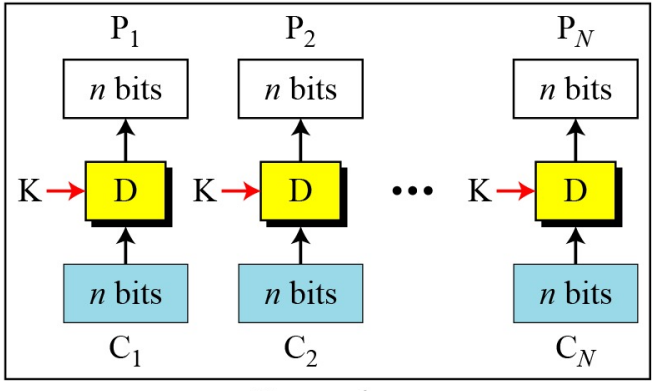


Electronic Code Book (ECB) mode (1)

- ECB mode



Encryption



Decryption

- Security issues:
  - Patterns of plaintexts are preserved
    - Same plaintexts lead to same ciphertexts
  - Attacker can exchange C_i blocks without knowing key K

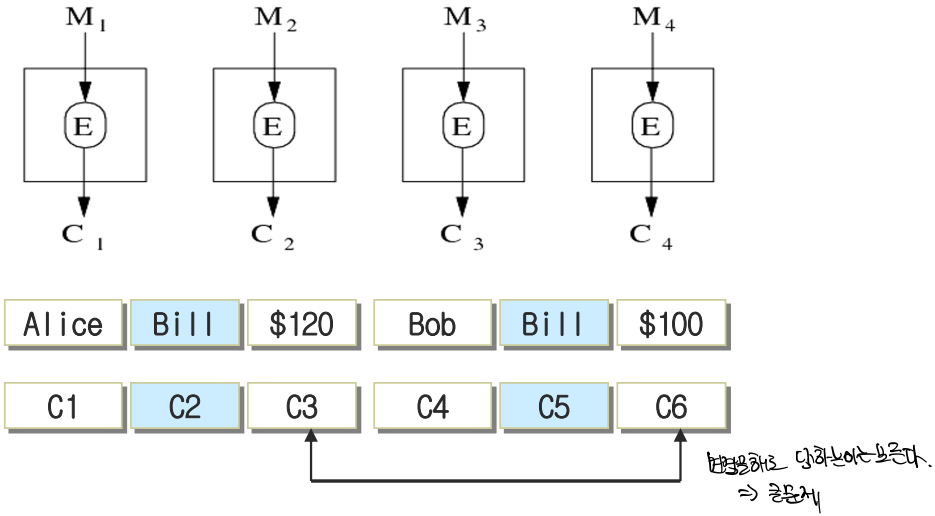

Original


Encrypted using ECB mode

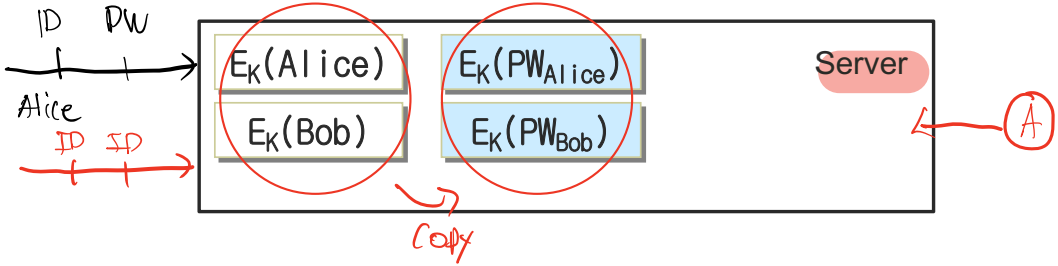

Encrypted using other modes

Electronic Code Book (ECB) mode (2)

- Examples of attacking ECB mode
  - In payment file system

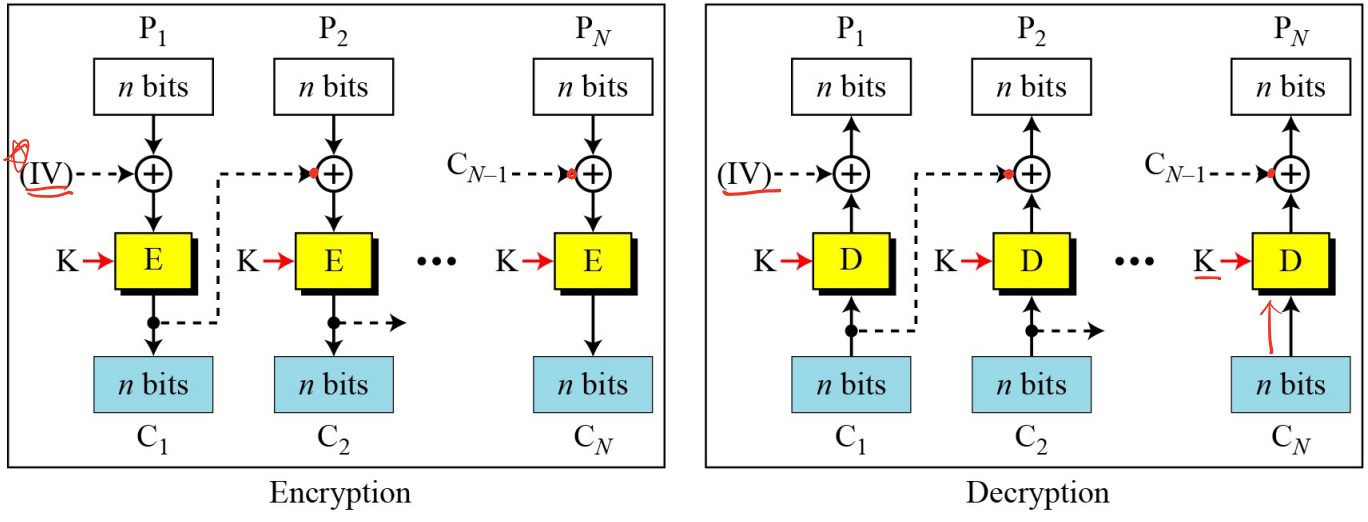


  - In ID/Password storage system(misguided example)



Cipher Block Chaining (CBC) mode(1)

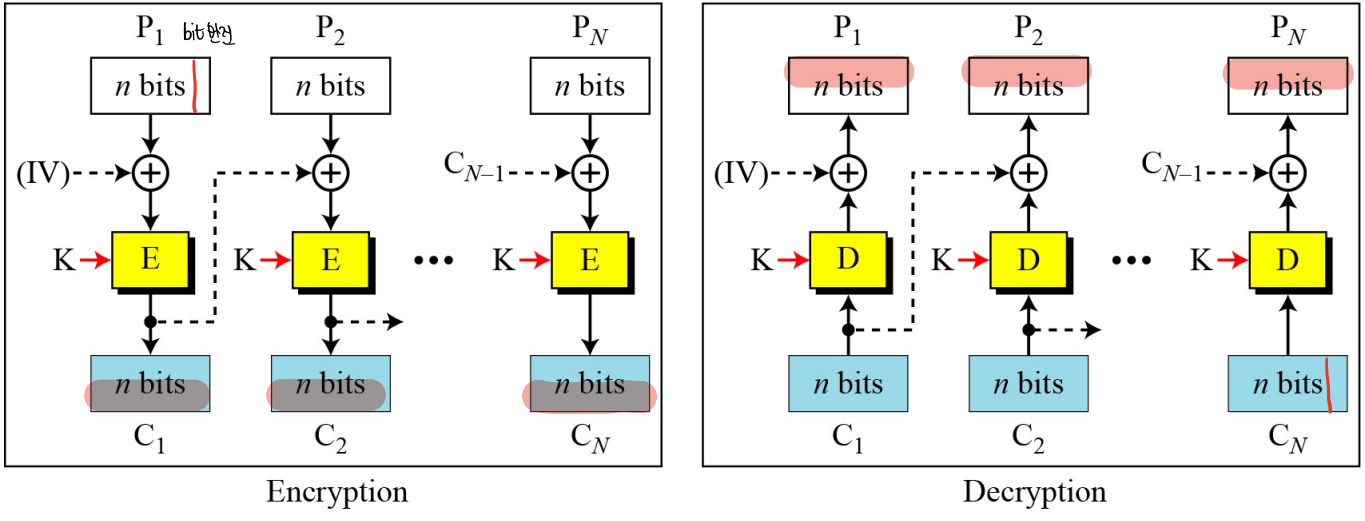
- CBC mode



  - Ciphertext = (IV, C_1, C_2, …, C_N)
  - IV (initial vector) is chosen at random (randomized algorithm)
    - Same plaintexts lead to distinct ciphertexts
    - Ciphertext must be longer than plaintext : CT-size = PT-size + |IV|
  - Drawback is that encryption must be carried out *sequentially*

Cipher Block Chaining (CBC) mode (2)

- Error propagation on CBC mode

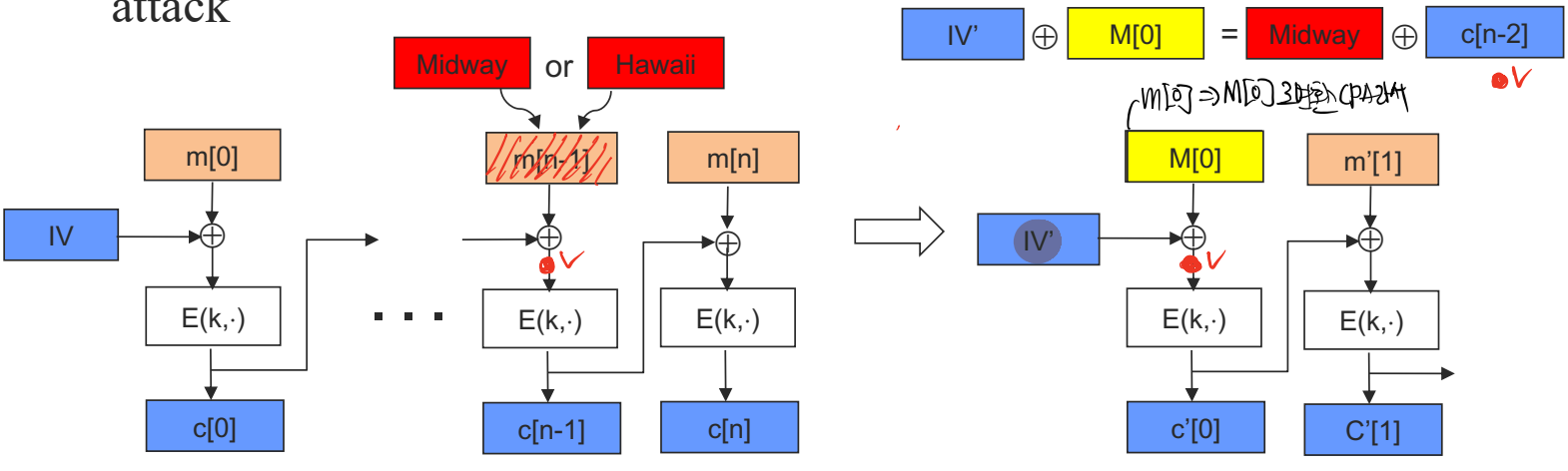


  - What if a single bit error occurs in a plaintext (during encryption)?
    - The error is propagated
    - Can be used for Message Authentication Code (MAC)
  - What if a single bit error occurs in a ciphertext (during transmission)?

Cipher Block Chaining (CBC) mode (3)

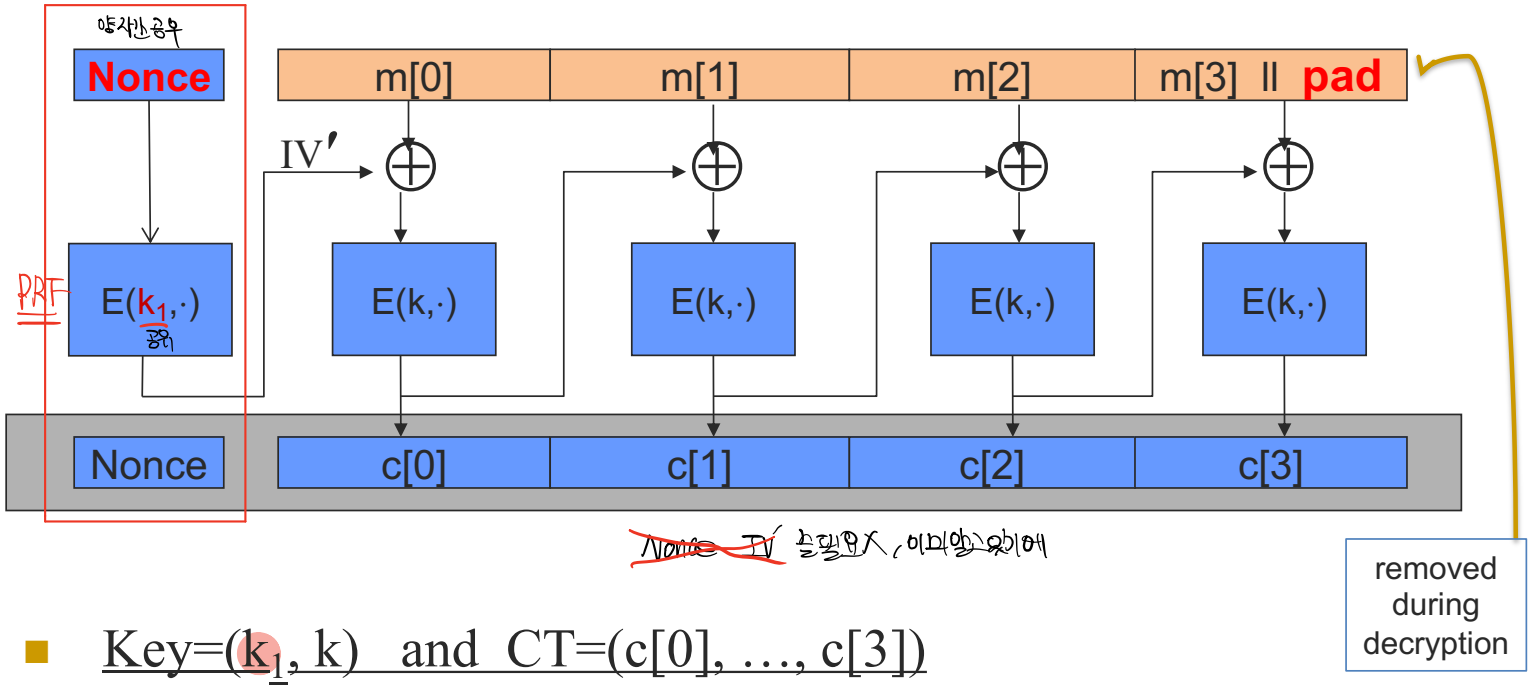
- Warning: IV should be chosen at random in every encryption
  - Attacker who can predict the IV can break CPA security!
  - Similarly applied to the case when the same IV is used

- Suppose (1) A can predict IV for next message (2) A does CPA attack



- Bug in SSL/TLS 1.0
  - IV for record #i is last CT block of record #(i-1)

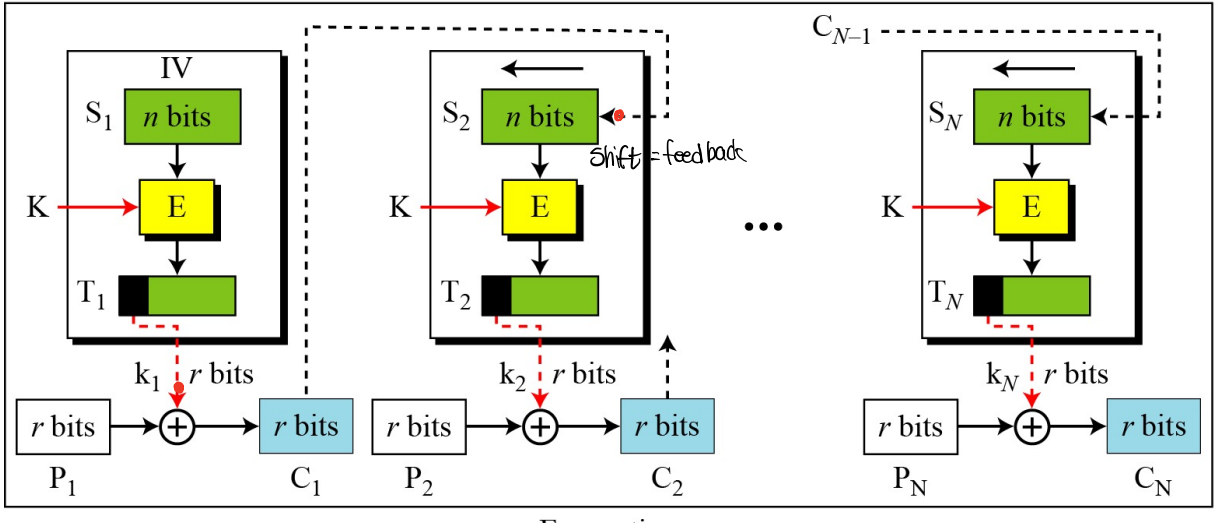
CBC technicality: Nonce-based



- Key=(k_1, k) and CT=(c[0], …, c[3])
- What is difference between CBC and the above one?
- TLS: byte padding is used (**pad =** n n n ••• n)
  - If no pad needed, add a dummy block

Cipher Feedback (CFB) mode

- CFB mode

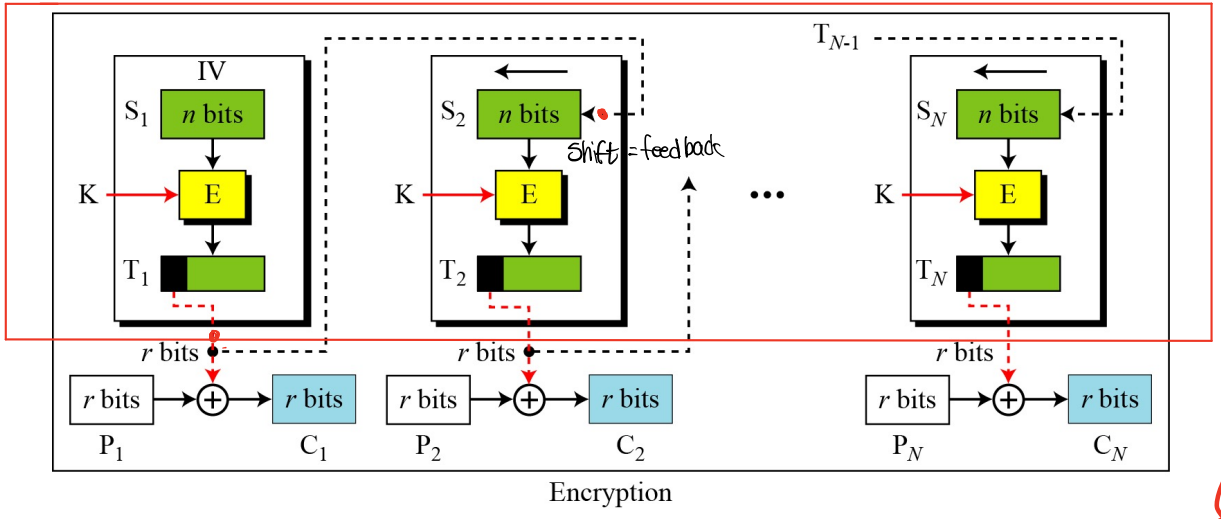


Encryption

  - Only *encryption* function is necessary
  - In some applications, block size gets smaller (e.g., ASCII 8-bit unit)
    - Less efficient than CBC mode (still sequentially)
  - How is error propagation in plaintext and ciphertext?

Output Feedback (OFB) mode

- OFB mode (as a stream cipher)



IV를 선택하면 key stream을 만들 수 있다.
= Stream Cipher.

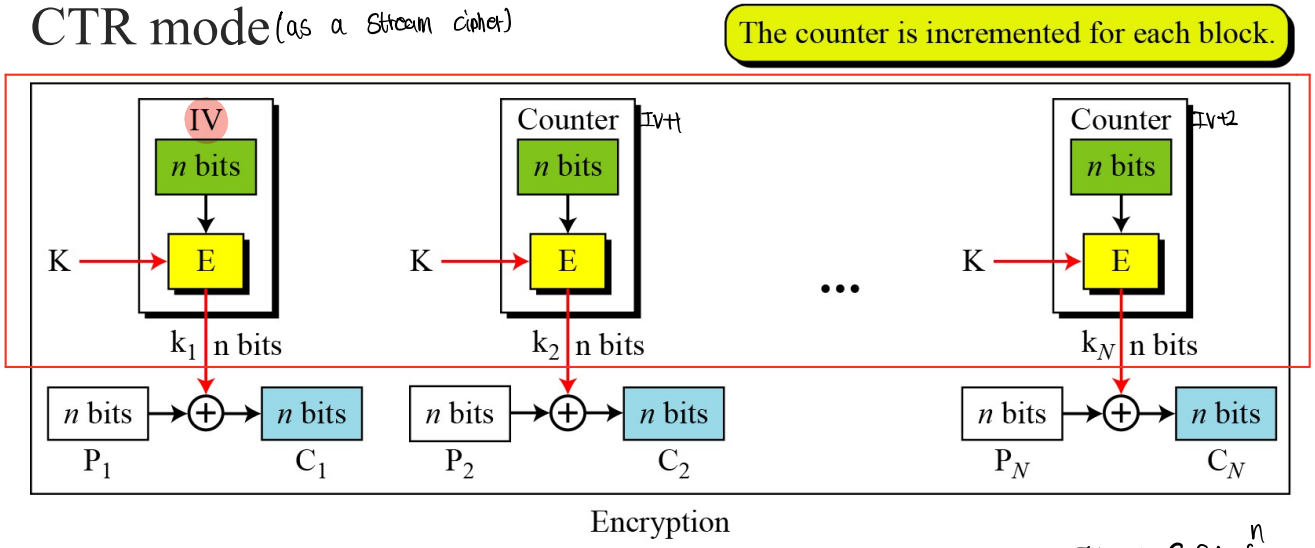
- Ciphertext = (IV, C_1, C_2, …, C_N)
- Only encryption function is necessary
  - Encryption(decryption) must be carried out sequentially
  - but, possible to prepare a stream in advance by using pre-processing
- How is error propagation in plaintext and ciphertext?

IV → $T_1, T_2 \cdots T_n$ key stream

대응되는 plaintext 에러.

Counter (CTR) mode

- CTR mode (as a stream cipher)



E = AES.

IV + 1 ∈ $\{0,1\}^n$

  - Ciphertext = (IV, C_1, C_2, …, C_N), where IV = CTR
    - IV ∈ $\{0,1\}^n$ is chosen at random
  - Only encryption function is used
    - Encryption (decryption) is fully parallelized
    - As with OFB, possible to generate a key stream in advance (key stream 미리 생성가능 = Stream cipher 처럼 동작.)
  - Possible to decrypt the i-th block C_i without decrypting any block (다른 블록과 관계없이.)

Comparison: CBC vs. CTR

		CBC	CTR
building block		PRP	PRF
as a stream cipher		No	Yes
parallel processing	Enc	No	Yes
	Dec	Yes	Yes
error propagation	Enc	Yes	No
	Dec	Two blocks	No
dummy padding block		Yes	No
1 byte msgs		16x expansion	no expansion

IV

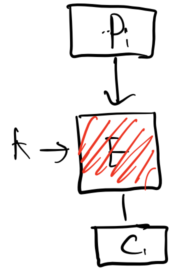
(for CBC, dummy padding block can be solved using ciphertext stealing)

nonce-based CBC / nonce-based CTR

Security Summary

- Among the five modes of operation
  - CBC, OFB, and CTR mode are secure (and suffice to use)
  - IV must be chosen at random per a new message
    - Same IV used can break encryption scheme
    - Security can be affected by IV, not key length and block length
  - Security result:

If F is a secure block cipher, then {CBC, OFB, CTR} is secure against chosen-plaintext attack



Enc에 의해 문제 발생할 수 있지만 운영모드에 의해 발생할 수 있다.

CPA

- Stated security result summarized in the following table:

CCA

Power / Goal	one-time key	Many-time key (CPA)	CPA and integrity
CPA Security	- Stream cipher - Determ. ctr-mode	CBC mode CTR mode	later

Q & A